CLAIMS

What is claimed is:

1. A method, comprising:

retrieving a first key from a secure store associated with a firmware within a platform, the firmware including an initialization table for initializing the platform; and

verifying the initialization table using the first key retrieved from the secure store during an initialization of the platform.

2. The method of claim 1, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the method further comprises:

retrieving a second key from the secure store; and

verifying at least one initialization segment using the second key retrieved from the secure store.

3. The method of claim 2, wherein the at least one initialization segment is signed using the second key prior to being stored in the firmware.

4. The method of claim 2, further comprising examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is performed only if the at least one initialization segment includes the code to be dispatched.

5. The method of claim 4, further comprising:

determining whether the verification is performed successfully; and

executing the code dispatched from the at least one initialization segment if the verification is performed successfully.

6. The method of claim 5, further comprising resetting the platform if the verification is performed unsuccessfully.

7. The method of claim 2, further comprising executing the at least one initialization segment without performing the verification, if the at least one initialization segment does not include the code to be dispatched.

8. The method of claim 1, wherein the initialization of the platform is performed during a resume process of the platform, and wherein the first and second keys are generated, and the initialization table and the at least one initialization segment are signed during a boot process of the platform.

9. A machine-readable medium having executable code to cause a machine to perform a method, the method comprising:

retrieving a first key from a secure store of a firmware within a platform, the firmware including an initialization table for initializing the platform; and

verifying the initialization table using the first key retrieved from the secure store during an initialization of the platform.

10. The machine-readable medium of claim 9, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the method further comprises:

retrieving a second key from the secure store; and

verifying at least one initialization segment using the second key retrieved from the secure store.

11. The machine-readable medium of claim 10, wherein the method further comprises examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is

performed only if the at least one initialization segment includes the code to be dispatched.

12. The machine-readable medium of claim 11, further comprising:
determining whether the verification is performed successfully; and
executing the code dispatched from the at least one initialization segment if the verification is performed successfully.

13. A data processing system, comprising:
a processor;
a memory coupled to the processor to store an initialization table for initializing the data processing system, the memory including a secure store; and
a process, when executed from the memory, causes the processor to
retrieve a first key from the secure store, and
verify the initialization table using the first key retrieved from the secure store during an initialization of the data processing system.

14. The data processing system of claim 13, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the process further causes the processor to:
retrieve a second key from the secure store; and
verify at least one initialization segment using the second key retrieved from the secure store.

15. The data processing system of claim 14, wherein the process further causes the processor to examine the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is performed only if the at least one initialization segment includes the code to be dispatched.

16. A method, comprising:

generating a first key to sign an initialization table of a firmware in a platform, the initialization table being used to initialize the platform;

signing the initialization table using the first key;

storing the first key in a secure store of the firmware; and

locking the secure store after the first key is stored in the secure store.

17. The method of claim 16, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the method further comprises:

generating a second key;

signing at least one initialization segment of the initialization table using the second key; and

storing the second key in the secure store prior to locking the secure store.

18. The method of claim 17, further comprising examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the signing operations using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

19. The method of claim 16, wherein the first and second keys are generated, and the initialization table and the at least one initialization segment are signed during a boot process of the platform.

20. A machine-readable medium having executable code to cause a machine to perform a method, the method comprising:

generating a first key to sign an initialization table of a firmware in a platform, the initialization table being used to initialize the platform;

signing the initialization table using the first key;

storing the first key in a secure store of the firmware; and

locking the secure store after the first key is stored in the secure store.

21. The machine-readable medium of claim 20, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the method further comprises:

generating a second key;

signing at least one initialization segment of the initialization table using the second key; and

storing the second key in the secure store prior to locking the secure store.

22. The machine-readable medium of claim 21, wherein the method further comprises examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the signing operation using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

23. A data processing system, comprising:

a processor;

a memory coupled to the processor to store an initialization table for initializing the data processing system, the memory including a secure store; and

a process, when executed from the memory, causes the processor to

generate a first key to sign the initialization table,

sign the initialization table using the first key,

store the first key in the secure store, and

lock the secure store after the first key is stored in the secure store.

24. The data processing system of claim 23, wherein the initialization table comprises one or more initialization segments that are individually executable, and wherein the process further causes the processor to:

generate a second key,

sign at least one initialization segment of the initialization table using the second key, and

store the second key in the secure store prior to locking the secure store.

25. The data processing system of claim 24, wherein the process further causes the processor to examine the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the signing operation using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

26. An apparatus, comprising:

an initialization engine to carry out operations of an initialization table for initializing a platform;

a secure store to perform one or more keys for signing at least a portion of the initialization table; and

a verifier coupled to the initialization engine and the secure store to verify at least a portion of the initialization table using at least one of the one or more keys during an initialization of the platform.

27. The apparatus of claim 26, wherein the one or more keys include a first key, and wherein the initialization engine generates the first key and signs at least a portion of the initialization table using the first key during a boot time of the platform.

28. The apparatus of claim 26, wherein the initialization table includes one or more initialization segments that are individually executable, wherein the one or more keys

include one or more second keys generated for signing the one or more initialization segments respectively during a boot time of the platform.

29. The apparatus of claim 26, wherein during a resume time of the platform, the verifier retrieves the first key from the secure store and verifies the initialization table using the first key.

30. The apparatus of claim 29, wherein for each of the initialization segments that have been signed, the verifier further retrieves the second keys and verifies the signed initialization segments using the second keys respectively.